

**REMARKS**

This Application has been carefully reviewed in light of the Office Action mailed March 11, 2005. Claims 1-15 were pending in the Application. In the Office Action, Claims 1-15 were rejected. Claims 1-15 remain pending in the Application. Applicants respectfully request reconsideration and favorable action in this case.

**CLAIM 12**

In the Office Action, the Examiner never explicitly refers to Claim 12 other than indicating that Claim 12 is rejected on page 1 of the Office Action. Thus, the Examiner does not appear to provide any basis or reasoning as to why Claim 12 is rejected or what the statutory basis is for rejecting Claim 12. Accordingly, Applicants are unable to adequately respond to any such rejection of Claim 12 if Claim 12 is indeed rejected. Therefore, Applicants respectfully request that the Examiner provide the required bases if the Examiner is maintaining a rejection of Claim 12 and request that any subsequent Office Action be made **non-final** so that Applicants may address any such rejection of Claim 12.

In the Office Action, the following actions were taken or matters were raised:

**SPECIFICATION OBJECTIONS**

The Examiner suggested that Applicants provide the serial numbers of related co-pending applications mentioned on page 1 of the specification. Applicants have so amended the indicated related applications portion of the specification to include such serial numbers. Favorable action is respectfully requested.

**SECTION 102 REJECTIONS**

The Office Action indicates that only Claim 1 is rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent No. 6,279,113 issued to Vaidya (hereinafter "*Vaidya*"). However, in the Office Action, under the discussion of the 35 U.S.C. 102(e) rejection, the Examiner also refers to Claims 2-5 and 13-15. Accordingly, Applicants presume that the Examiner meant to reject Claims 1-5 and 13-15 under this 35 U.S.C. 102(e) rejection in view

of *Vaidya*, and Applicants respond based on the foregoing. Applicants respectfully traverse this rejection.

“A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference.” *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 U.S.P.Q.2d 1051, 1053 (Fed. Cir. 1987) (emphasis added); MPEP 2131. Additionally, “[t]he identical invention must be shown in as complete detail as is contained in . . . the claim.” *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 1236, 9 U.S.P.Q.2d 1913, 1920 (Fed. Cir. 1989) (emphasis added); MPEP 2131.

Independent Claim 1 recites, at least in part, “a network stack comprising a protocol driver, a media access control driver and an instance of the intrusion prevention system implemented as an intermediate driver and bound to the protocol driver and the media access control driver.” In the Office Action, the Examiner refers generally to column 6, lines 11-18, column 7, lines 12-24, and figure 2 of *Vaidya* as disclosing the above-references limitation(s) (Office Action, page 3). However, Applicants respectfully submit that the above-referenced limitation(s) are not disclosed or even suggested in the portions of *Vaidya* referred to by the Examiner or elsewhere in *Vaidya*. For example, *Vaidya* does not appear to disclose or even suggest a network stack as recited by independent Claim 1 (e.g., “a protocol driver, a media access control driver and an instance of the intrusion prevention system implemented as an intermediate driver”), nor has the Examiner explicitly identified any such disclosure in the *Vaidya* reference. Thus, the Examiner has not established a *prima facie* case of anticipation of independent Claim 1 at least because *Vaidya* does not disclose or even suggest “[t]he identical invention . . . in as complete detail as is contained in . . . the claim,” nor has the Examiner provided any of the required reasoning or bases to support the rejection of Claim 1 pursuant to the courts and the M.P.E.P. Therefore, Applicants respectfully submit the rejection of Claims 1 is improper and should be withdrawn.

Independent Claim 13 recites, at least in part, “determining a correspondence between the packet and at least a subset of the plurality of machine-readable network-exploit signatures” (emphasis added). Regarding Claim 13, the Examiner refers to column 6, line 57,

through column 7, line 6, of *Vaidya* as disclosing the limitations of independent Claim 13. Applicants respectfully disagree. *Vaidya* appears to disclose a configuration builder module 32 that assigns a set of signature profiles to each network object and stores data representative of associations between network objects and attack signature profile sets in a signature profile memory 39 (*Vaidya*, column 6, lines 3-7). *Vaidya* also appears to disclose a data collector 10 that monitors network data to detect packets addressed to network objects on the network segment on which the data collector 10 is located, and when the data collector 10 detects a data packet addressed to a network object having an associated attack signature profile set in the signature profile memory 39, the data collector accesses the attack signature profile set and processes attack signature profiles to determine if the packet is associated with a network intrusion (*Vaidya*, column 6, line 57, to column 7, line 2). Thus, *Vaidya* appears to disclose that in response to determining that a packet is addressed to particular network object, the packet is compared to the attack signatures contained in the set of signatures associated with that particular network object. Accordingly, *Vaidya* does not appear to disclose or even suggest that the packet matches or corresponds to “at least a subset of the plurality of machine-readable network-exploit signatures” as recited by Claim 13 (emphasis added). To the contrary, the “set” of attack signatures in *Vaidya* is associated with a particular network object and appears only to comprise those signatures with which the packet is compared. Thus, for at least this reason, Applicants respectfully submit that *Vaidya* does not anticipate Claim 13.

Claims 2-5, 14 and 15 that depend from respective independent Claims 1 and 13 are also not anticipated by *Vaidya* at least because they incorporate the limitations of respective Claims 1 and 13 and, also, they add additional elements that further distinguish *Vaidya*. Therefore, Applicant respectfully requests that the rejection of Claims 2-5, 14 and 15 be withdrawn.

### **SECTION 103 REJECTIONS**

The Office Action indicates that only Claim 6 is rejected under 35 U.S.C. 103(a) as being unpatentable over *Vaidya* in view of U.S. Patent No. 6,578,147 issued to Shanklin et

al. (hereinafter “*Shanklin*”). However, in the Office Action, under the discussion of the 35 U.S.C. 103(a) rejection, the Examiner also refers to Claims 7-11. Accordingly, Applicants presume that the Examiner meant to reject Claims 6-11 under this 35 U.S.C. 103(a) rejection in view of *Vaidya* and *Shanklin*, and Applicants respond based on the foregoing. Applicants respectfully traverse this rejection.

Of the rejected claims, Claim 6 is independent. Applicants respectfully submit that neither *Vaidya* nor *Shanklin*, alone or in combination, discloses, teaches or suggests the limitations of independent Claim 6. For example, Applicants respectfully submit that neither *Vaidya* nor *Shanklin*, alone or in combination, discloses, teaches or suggests “comparing the packet with a plurality of machine-readable network-exploit signatures” and “determining a correspondence between the packet and at least two of the plurality of machine-readable network-exploit signatures” as recited by Claim 6 (emphasis added).

In the Office Action, the Examiner admits that *Vaidya* does not explicitly show determining correspondence between the packet and at least two of the network-exploit signatures (Office Action, page 6). However, the Examiner states that *Shanklin* discloses an intrusion detection system that forwards packets from different sessions to a network analyzer to be used in detecting certain types of composite signatures, and that it would have been obvious to modify *Vaidya* with the teaching of *Shanklin* to arrive at Applicants’ Claim 6 (Office Action, pages 6-7). Applicants respectfully disagree.

The portion of *Shanklin* referred to by the Examiner in the Office Action states:

A network analyzer 25 receives packets from different sessions, which may be used to detect certain types of composite signatures. For example, a “ping” type signature is indicated by multiple sessions that attempt to connect to different destinations with the local network. Single packets indicating ping behavior can be delivered to network analyzer 25, which then monitors similar packets from different sessions to see if a ping pattern is indicated. In general, network analyzer 25 detects signatures of attacks against multiple hosts and different sessions. Such attacks are often detecting using statistical correlations.

(*Shanklin*, column 5, lines 29-39). Applicants respectfully submit that monitoring packets from different sessions is not equivalent to “determining a correspondence between [a] packet and at least two of the plurality of machine-readable network-exploit signatures” as recited by Claim 6 (emphasis added) which is clearly not disclosed or even suggested by the portion of *Shanklin* referred to by the Examiner or elsewhere in *Shanklin*. Further, as apparently recognized by the Examiner, *Vaidya* does not remedy at least this deficiency of *Shanklin*. Accordingly, Applicants respectfully submit that neither *Vaidya* nor *Shanklin*, alone or in combination, discloses, teaches or suggests the limitations of independent Claim 6. Therefore, Applicants respectfully request that the rejection of Claim 6 be withdrawn.


Claims 7-11 depend from independent Claim 6. For at least the reasons discussed above, independent Claim 6 is patentable over the cited references. Therefore, Claims 7-11 that depend therefrom are also patentable, and Applicants respectfully request that the rejection of Claims 7-11 be withdrawn.

**CONCLUSION**

Applicants have made an earnest attempt to place this case in condition for immediate allowance. For the foregoing reasons and for other reasons clearly apparent, Applicants respectfully request reconsideration and full allowance of all pending claims.

No fee is believed due with this Response. If, however, Applicant has overlooked the need for any fee due with this Response, the Commissioner is hereby authorized to charge any fees or credit any overpayment associated with this Response to Deposit Account No. 08-2025 of Hewlett-Packard Company.

Respectfully submitted,

By:   
James L. Baudino  
Reg. No. 43,486

Date: June 10, 2005

Correspondence to:  
L.Joy Griebenow  
Hewlett-Packard Company  
Intellectual Property Administration  
P. O. Box 272400  
Fort Collins, CO 80527-2400  
Tel. 970-898-3884